First Iteration – Provision of Final Safety Assessment Report

Document information	
Project title	Surveillance ground system enhancements for ADS-B (Prototype development)
Project N°	15.04.05b
Project Manager	Thales Air Systems
Deliverable Name	First Iteration – Provision of Final Safety Assessment Report
Deliverable ID	D08
Edition	00.02.00
Template Version	02.00.00
Task contributors	
NATS, EUROCONTROL, INDRA, SELEX, THALES, NORACON	

Abstract

SESAR WP15.4.5 is tasked with the implementation of enhancements into the ADS-B ground based surveillance system to address known security limitations of ADS-B technology. It is planned that the enhanced ADS-B ground system will offer a sufficiently robust service so that it can augment existing radar surveillance services within ATS controlled airspace.

WP15.4.5b will develop three pre-industrialisation prototypes of the enhanced ADS-B ground system, termed Prototype First, Second or Third Iteration.. The enhanced ADS-B ground system will comprise interconnected remote ADS-B groundstations, an optional WAM system input and an SDPD system. ADS-B target information is validated by the implemented security enhancements and the validation results passed to the SDPD for processing within the Multi-Sensor Tracker.

This safety report provides a safety assessment of the Prototype First Iteration of the enhanced ADS-B ground system. It assesses the Safety, Performance and Requirements standard document for each of the ADS-B applications which the first iteration prototype has been defined to address. It describes the deltas between the logical model presented within the current standards and what extension would be required to incorporate the enhanced ADS-B ground system elements.

Examples of the approach to analyse the new logical model are presented and hence the reader is informed of the current situation, determined through consultation with Safety Subject Matter Experts and therefore it is proposed that this report can act as an input into the EUROCONTROL Generic Surveillance SPR standard drafting process and the composite ADS-B & WAM work being conducted by EUROCAE.

Authoring & Approval

Prepared By		
Name & company	Position / Title	Date
[redacted] NATS	[redacted]	15/05/2012

Reviewed By		
Name & company	Position / Title	Date
[redacted] THALES	[redacted]	09/05/2012
[redacted] INDRA		04/05/2012
[redacted] NORACON		04/05/2012
[redacted] SELEX		04/05/2012
[redacted] EUROCONTROL		09/05/2012
[redacted] EUROCONTROL		09/05/2012
[redacted] NATS		09/05/2012
[redacted] NATS		09/05/2012

Approved By		
Name & company	Position / Title	Date
[redacted] THALES	[redacted]	15/05/2012
[redacted] INDRA		15/05/2012
[redacted] NORACON		16/05/2012
[redacted] SELEX		17/05/2012
[redacted] EUROCONTROL		16/05/2012

Document History

Edition	Date	Status	Author	Justification
00.00.01	28/03/2012	Draft	[redacted]	New Document
00.01.00	30/04/2012	Issued		Formal document
00.02.00	15/05/2012	Issued		Edition 00.02.00 to address EUROCONTROL comments against Edition 00.01.00

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

1.0 Executive summary

SESAR WP15.4.5 is tasked with the implementation of enhancements into the ADS-B ground based surveillance system to address known security limitations of the core ADS-B technology. It is planned that the enhanced ADS-B ground system will be offer a sufficiently robust service so that it augments existing radar services within ATS controlled airspace.

WP15.4.5b will develop three pre-industrialisation prototypes of the enhanced ADS-B ground system, termed Prototype First, Second or Third Iteration. Each Iteration corresponds to a separate SESAR CONOPS and Prototype First Iteration is aligned with SESAR Time Based Operations CONOPS. The enhanced ADS-B ground system will comprise remote enhanced ADS-B groundstations connected to an enhanced SDPD system, via modified ASTERIX interfaces.

This safety report assesses the EUROCAE Safety, Performance and Requirements standard document for the ADS-B RAD [3], ATSA-ITP [6], ATSA-VSA [7] and ATSA-AIRB [8] applications and concludes that they placed no Safety Requirements on the ADS-B Ground System. ATSA-VSA assumes however the presence of a radar (independent from ADS-B) and would this not be case at implementation level, then a specific safety assessment should be undertaken (e.g. at local level) to cover the possible case of common mode of failure between airborne and ground surveillance..

The ADS-B RAD application is supported by the first iteration prototype and hence its SPR document was assessed to have direct impact on the Enhanced ADS-B Ground System and assessed in detail [3]. The SPR process is described, starting with the Operational Scenario and Environment Definition (OSED), featuring the ADS-B RAD Environment Scenarios and Surveillance Functional Model. The Separation Standards Error analysis and Operational Performance Assessment are summarised and they represent the ‘success’ case for the application safety analysis.

The ADS-B RAD Operational Safety Assessment process is then described in detail, featuring an Operational Hazard Assessment (OHA) and an Allocation of Safety Objectives and Requirements (ASOR) activity. The OSA represents the ‘failure’ case for the application safety analysis. The report concludes by an assessment of the applicability of the ADS-B RAD SPR standard to a surveillance scenario incorporating the Enhanced ADS-B Ground System. It describes the necessary modifications to the ADS-B RAD Surveillance Functional Model to incorporate elements of the Enhanced ADS-B Ground System.

The report concludes that a full Operational Hazard assessment with the new Surveillance Functional Model should be undertaken, as the enhancements introduced into the Prototype First Iteration system may have the potential to add new Operational Hazards or add new Basic Causes to the existing fault trees within the ADS-B RAD standard. If through assessment it was found that the enhancements have added new operational hazards to the OH set defined within the RAD standard then these would require event tree and fault trees to be created for each hazard., thereby enabling a full set of Safety Requirements to be defined for the Enhanced ADS-B Ground System.

It is proposed that this document could act as an input into the EUROCAE "Composite" work (ADS-B/WAM Ground Station) and to the EUROCONTROL Generic Surveillance (GEN-SUR) SPR standard being currently developed.

2.0 Introduction

2.1 Purpose of the document

This safety assessment assesses the input ADS-B standards defined within the enhanced ADS-B ground station specification for Prototype Iteration One and determines which standard is relevant to the enhanced ADS-B ground system.

2.2 Intended readership

The audience of this document includes:

- Projects 15.04.05 a and b,
- SJU projects that may require ADS-B Surveillance Systems for their validation activities.

2.3 Inputs from other projects

Input documents in the form of system specifications, interface specifications and test specifications for the enhanced ADS-B ground system from WP15.4.5a. Industry standards and Preliminary Safety Case studies also provide input material.

2.4 Structure of the document

- Chapter 1: Executive Summary
- Chapter 2: Introduction
- Chapter 3: Project Structure and Deliverables per Iteration
- Chapter 4: Airborne and Ground Surveillance ADS-B Applications
- Chapter 5: Package 1 ADS-B Applications
- Chapter 6: Airborne Surveillance ATSA Applications
- Chapter 7: Ground Surveillance ADS-B Applications
- Chapter 8: Applicability of the ADS-B RAD SPR Standard to the 15.4.5 Enhanced ADS-B Ground System
- Chapter 9: References
- Chapter 10. Appendix A

2.5 Acronyms and Terminology

Term	Definition
ADS-B	Automatic Dependent Surveillance - Broadcast
ADS-B$_{IN}$	"ADS-B in" application
ADS-B$_{OUT}$	"ADS-B out" application
ADS-B-APT	ADS-B Airport Surface Surveillance Application
ADS-B NRA	Enhanced Air Traffic Services in Non-Radar Areas using ADS-B surveillance
ADS-B RAD	Enhanced Air Traffic Services in Radar-Controlled Areas using ADS-B surveillance
ARTAS	ATM suRveillance Tracker And Server
ASAS	Airborne Separation Assurance System
ASPA	Airborne SPAcing
ASEP	Airborne SEParation
ASOR	Allocation of Safety Objectives and Requirements
ASSUMP	Assumption
ASTERIX	All-purpose Structured EUROCONTROL Surveillance Information Exchange
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATS	Air Traffic Services
ATSA	Airborne Traffic Situational Awareness
ATSA-AIRB	Airborne Traffic Situational Awareness "Enhanced Traffic Situational Awareness During Flight Operations"
ATSA-ITP	Airborne Traffic Situational Awareness "In Trail Procedures"
CAT	Data Category
CWP	Controller Working Position

Term	Definition
DO	RTCA Safety Performance Requirements Standard document
EC	Environmental Condition
ED	EUROCAE Safety Performance Requirements Standard document
EMM	External Mitigation Means
ES	Environment Scenarios
EUROCAE	European Organisation for Civil Aviation Equipment
GS	Ground Surveillance
INTEROP	Interoperability
IMM	Internal Mitigation Means
IR	Interoperability Requirement
Mode S	Mode Select
MST	Multi-Sensor Tracker
NACp	Navigation Accuracy for Position
NIC	Navigation Integrity Category
OH	Operational Hazard
OHA	Operational Hazard Assessment
OPA	Operational Performance Assessment
OR	Operational Requirement
OSA	Operational Safety Assessment
OSED	Operational Service and Environment Definition
Pe	Probability of Effect
PO–ASAS	Principles of Operation for the use of Airborne Separation Assurance Systems
PR	Performance Requirement
RFG	Requirement Focus Group
RTCA	Radio Technical Commission for Aeronautics

Term	Definition
SDPD	Surveillance Data Processing and Distribution
SESAR	Single European Sky ATM Research (Programme)
SJU	SESAR Joint Undertaking
SR	Safety Requirement
SPR	Safety and Performance Requirements
SPR-INTEROP	Safety, Performance and Interoperability Requirements
SSE	Surveillance Separation Error
SSEP	Self SEParation
SSR	Secondary Surveillance Radar
TIS	Traffic Information Service
TMA	Terminal Manoeuvring Area
WAM	Wide Area Multilateration
WP	Work Package

3.0 Project structure & deliverables per Iteration

WP15.4.5 is tasked with the production of three technology demonstrator level prototype enhanced ADS-B ground system. The boundaries of the Enhanced ADS-B ground system were defined within the ADS-B Ground Surveillance Specification for First Iteration to include the elements shown in blue in Figure 1[16]:

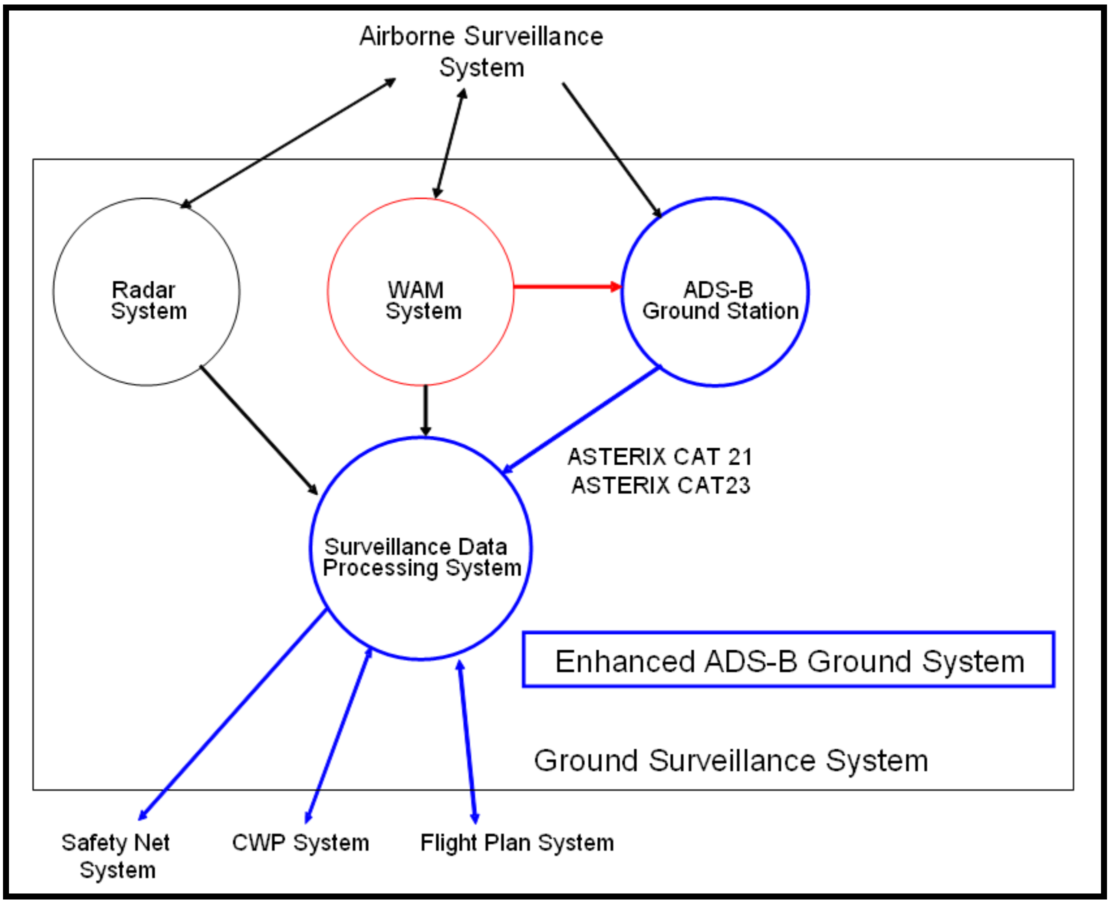

Figure 1. Enhanced ADS-B ground system boundaries

SESAR WP15.4.5 project is split into two parts; 15.4.5a and 15.4.5b

- 15.4.5a provides the system specifications and test specification for each iteration of the project. Specifications provided include the Specification Baseline document which defines the supported ADS-B operational applications for each prototype iteration and the security enhancements planned to be integrated into each iteration, the enhanced ADS-B ground system specification, the enhanced ADS-B groundstation system specification, the enhanced SDPD system specification, the ADS-B Ground Surveillance System interface modification specifications and system test specification.
- 15.4.5b takes the input specification set from the 'a' project for each iteration, defines the baseline requirements matrix of the prototype iteration of the enhanced ground system, develops the prototype system elements against this baseline and performs the specified tests against the developed prototype to demonstrate this correct implementation of these requirement.

This report is the Task 08 deliverable within Prototype First Iteration of the enhanced ADS-B ground system.

4.0 Airborne and Ground Surveillance ADS-B Applications

To progress the formulation and standardisation of ADS-B applications EUROCONTROL and the FAA formed a joint EUROCAE and RTCA activity termed the ADS-B 'Requirements Focus Group' or ADS-B RFG, which assumed the responsibility for the production of formal ADS-B application standards.

The ADS-B RFG divided ADS-B operational applications into two categories [1];

a) use of ADS-B by aircraft, termed Airborne Surveillance (AS) applications,

b) use of ADS-B by Air Traffic Services (ATS), termed Ground Surveillance (GS) applications.

4.1 Assumed Aircraft and Ground Generic Functional Architecture

To facilitate the development of common application standards the ADS-B RFG formulated a generic Surveillance Functional Architecture model to support all of the defined Package 1 Airborne Surveillance or Ground Surveillance ADS-B applications e.g. [2]-[3], [6]-[8]:

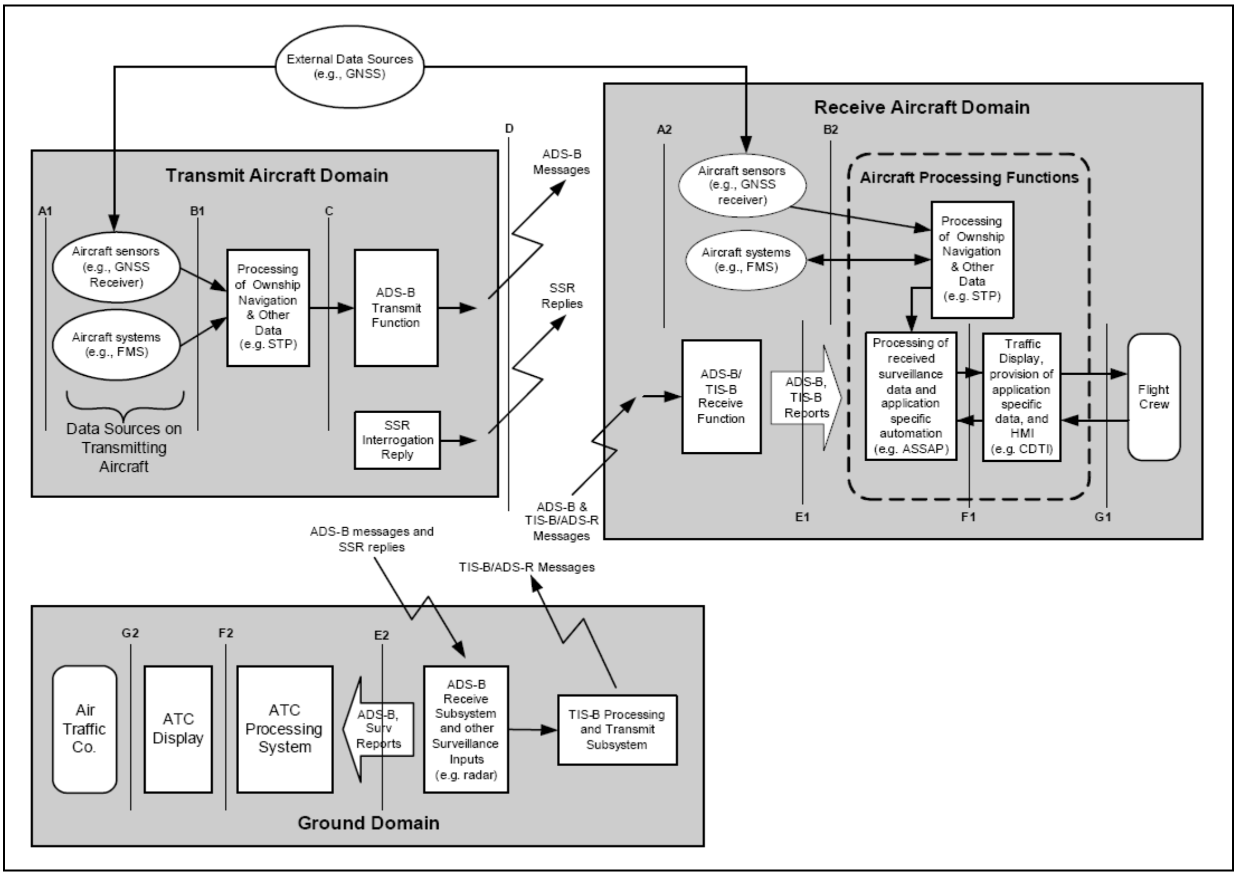

Figure 2. Generic RFG Surveillance Functional Architecture model

The RFG model shows the Transmit Aircraft and Receive Aircraft domain boundaries and the Ground Domain boundaries, the surveillance functions contained which each domain and the defined interfaces between the domains i.e. A1, B1, C within the Transmit Aircraft Domain; D between the Transmit Aircraft and Receive Aircraft and Ground Domains; A2, B2, E1, F1, G1 within the Receive Aircraft Domain; E2, F2, G2 within the Ground Domain.

4.2 Airborne Surveillance applications

Airborne Surveillance applications are concerned with the broadcast of ADS-B messages from the ‘Transmit Aircraft Domain’, and reception and display of ADS-B messages to the Flight Crew in the ‘Receive Aircraft Domain’ (Figure 2). Airborne Surveillance applications are primarily aimed at improving the flight crew situational awareness and due to location of the ADS-B information usage within the Aircraft Domains these applications are commonly referred to as **ADS-B$_{IN}$** applications.

Airborne Surveillance ADS-B applications have been defined to have the following sub-categories, with further details given in Appendix A;

- Airborne Separation Assistance Services: ASAS [1]
- Airborne Traffic Situational Awareness: PO-ASAS category I or ATSA [1]
- Airborne Spacing: PO-ASAS category II or ASPA [1]
- Airborne Separation: PO-ASAS category III [1] or ASEP
- Airborne Self Separation: PO-ASAS category IV [1] or SSEP

Examples of Airborne Surveillance ADS-B applications include ATSA-ITP [6], ATSA-VSA [7] and ATSA-AIRB [8], ATSA-SURF [19] and ASPA-FIM [20]. Further details on ADS-B AS applications are given in Section 5.0.

4.3 Ground Surveillance Applications

Ground Surveillance (GS) ADS-B applications are concerned with improved ATS services through the broadcast of ADS-B messages by the ‘Transmit Aircraft Domain’ and the reception and display of ADS-B messages to Air Traffic Control Officers (ATCO) in the ‘Ground Domain’ (Figure 2).

ATC operational usage of ADS-B data is therefore within located the Ground domain in this type of application and hence they are commonly referred to as **‘ADS-B$_{OUT}$’** applications, due to the broadcast nature of the ADS-B information from the aircraft domain to the ground domain surveillance reception function and presentation to the controlling ATCO.

Examples of Ground Surveillance ADS-B applications include ADS-B NRA [2], ADS-B RAD [3] and ADS-B APT [18]. Further details on ADS-B GS applications are given in Section 5.0.

5.0 Package 1 ADS-B Applications

To enable early implementation of selected ADS-B applications and coordinate the necessary evolutionary changes to the airborne equipment and ground surveillance architecture, the ADS-B RFG grouped the more mature AS and GS ADS-B applications together and collectively termed them 'Package 1' applications [1].

Package 1 defined GS and AS ADS-B applications are given in the following list:

- **ADS-B NRA** Enhanced Air Traffic Services through the use of ADS-B data in areas where radar surveillance does not exist. ADS-B GS service defined to be similar to that provided by an SSR service [2].
- **ADS-B RAD** Enhanced Air Traffic Services in radar airspace using ADS-B surveillance. ADS-B GS service will support and in certain situations enhanced ATS provision in-addition to the existing radar services [3].
- **ADS-B APT** ADS-B GS service to provide or enhance existing surveillance services on airport surfaces to facilitate safer and more efficient ground movement management at airports [18].
- **ADS-B ADD** ADS-B GS service to provide aircraft FMS derived data (ADD) through ADS-B for use within the ATC ground system safety net tools. This data is the equivalent of Mode S ADD which is delivered via Downlink Aircraft Data (DAP) [1].
- **ATSA-ITP** The use of ADS-B AS service to enhance Airborne Traffic Situational Awareness 'In Trial Procedures' between pairs of aircraft in Procedural Airspace, enabling the change of Flight Level of one aircraft via a climb-through or descend-though manoeuvre in a coordinated and controlled manner [6].
- **ATSA-VSA** The use of ADS-B AS service to enhance Airborne Traffic Situational Awareness 'Visual Separation on Approach' procedures for a pair of successive aircraft on final approach to an airport. VSA comprises a Basic Procedure and a Advanced Procedure [7].
- **ATSA-AIRB** The use of ADS-B AS service to enhance Airborne Traffic Situational Awareness during Flight Operations. ATSA-AIRB is defined to contribute to improve the safety of flight operations through the provision of traffic situation awareness information to the flight crew through a dedicated ADS-B_{IN} display [8].
- **ATSA-SURF** The use of ADS-B AS service to enhance Traffic Situational Awareness on the airport surface for both taxi and runway operations in all weather conditions. Objectives for the ATSA –SURF AS application are to improve safety and operations efficiency in all visibility conditions [19].
- **ATSA-S&A** The use of ADS-B AS service to enhance Airborne Traffic Situational Awareness through enhanced visual acquisition for 'See and Avoid'. ATSA-S&A application acts as an aid to flight crews to perform their collision avoidance task when separation services are not provided by ATC [1].

- **ASPA-S&M** The use of ADS-B AS service to redistribute tasks relating to sequencing and merging of traffic between controllers and air crew. This airborne spacing application objectives were increase capacity and reduce controller workload [1].
- **ASPA-C&P** The use of ADS-B AS service to enable controllers to issue 'Crossing and Passing' instructions to aircraft to resolve potential aircraft conflicts, hence reducing controller workload [1].

Note: ADS-B-RAD is a combination of the former ADS-B-ACC (Area Control Centre) and ADS-B-TMA (Terminal Control Area) which defined ATC services based on ADS-B in en-Route and terminal areas, respectively in Package 1.

Note: ATSA-AIRB has been combined with the Package 1 definition of ATSA-S&A ("Enhanced Visual Acquisition for See-and-Avoid").

Note: ASPA-FIM is a set of functions and procedures defined to support a variety of airborne spacing operations, including the former ASPA-S&M (Sequencing and Merging) application.

Note: Enhanced Crossing and Passing Operations (ASPA-C&P), as defined in Package 1 has been dropped from the RFG work plan by RTCA SC-186 and EUROCAE WG51.

5.1 EUROCAE Safety, Performance and Interoperability Standards

The majority of the Package 1 ADS-B applications had an EUROCAE/RTCA standard document developed for them, following the methodology defined within ED-78A [4]. ED-78 states that each standard will feature an Operational Services and Environment Definition (OSED), an operational Safety and Performance Requirements (SPR) assessment and an Interoperability Requirements (INTEROP) assessment [4].

The sequence of the OSED, SPR and INTEROP activities within the production of an ED-78A compliant operational application standard is shown in Figure 3. It can be seen that the focus of the assessment changes from an operational ATS perspective towards a systems orientation throughout the course of the assessment, via several feedback loops. Through this iterative process the original OSED, SPR and INTEROP assessments become further refined to an finalised application SPR standard [3].

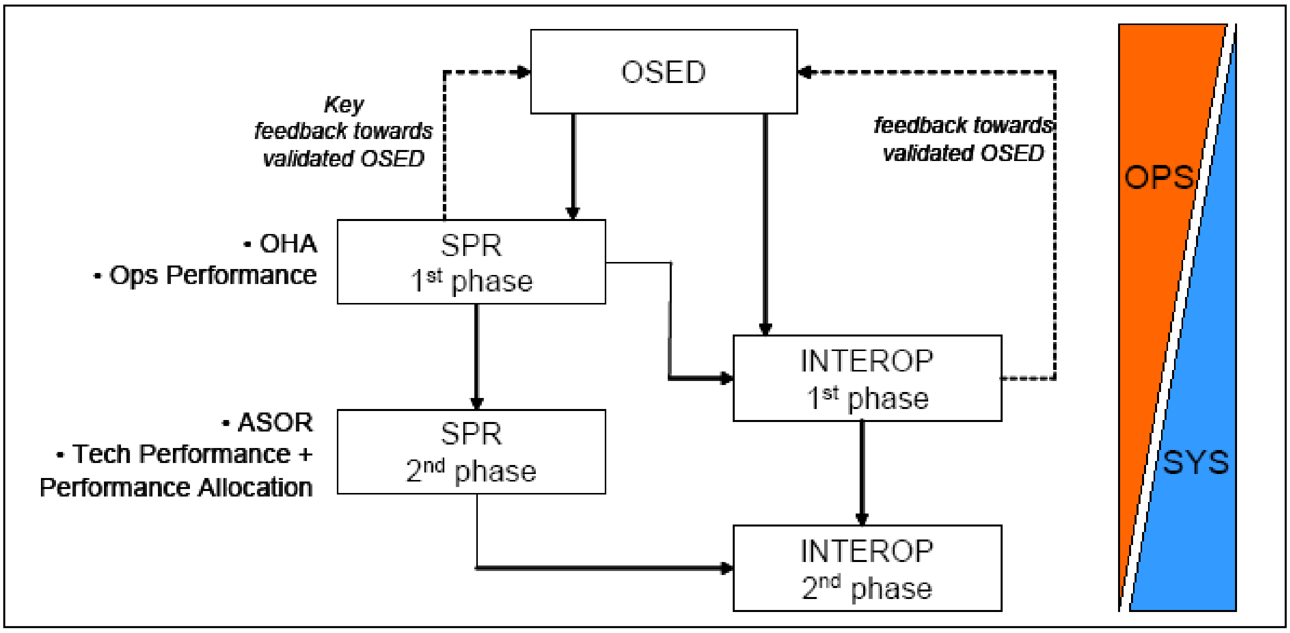

Figure 3. Operational standard production process following ED-78A

The generic Safety and Performance Requirements assessment is defined as [2]:

- An Operational Performance Assessment (OPA), which describes the system performance under nominal or no-fault conditions
- An Operational Safety Assessment (OSA), which describes the system performance under non-nominal or faulted conditions. The OSA is further sub-divided into:
  - Operational Hazard Assessment (OHA)
  - Allocation of Safety Objectives and Requirements (ASOR) activity.

A diagram illustrating the detailed SPR and INTEROP processes and generic requirement classification under ED-78A is shown in Figure 4 [8];

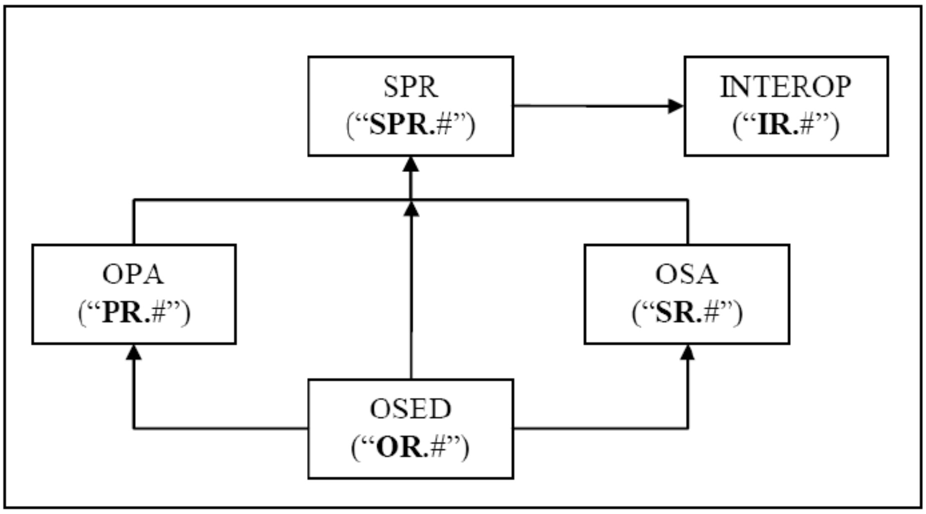

Figure 4. SPR and INTEROP requirements determination activities

OSED requirements are termed Operational Requirements and denoted by:	OR#
OPA requirements are termed Performance Requirements and denoted by:	PR#
OSA requirements are termed Safety Requirements and denoted by:	SR#
Safety Performance Requirements are denoted by:	SPR#
INTEROP requirements are termed Interoperability Requirements and denoted as:	IR#

5.2 15.4.5b Prototype First Iteration supported ADS-B applications

WP15.4.5b Prototype First Iteration of the enhanced ADS-B ground system has been defined within the 15.4.5.a Specification Baseline Document to address requirements from the following ADS-B 'Package 1' applications [9]:

- **ADS-B RAD**
- **ASTA ITP**
- **ASTA VSA**
- **ATSA AIRB**

Each one of these ADS-B applications has had an EUROCAE SPR standard document developed against it and these are listed in Table 1:

Item	ADS-B Application title	Category	SPR standard
1	**ADS-B RAD**	GS	**ED-161 [3]**
2	**ATSA ITP**	ATSA	**ED-159 [6]**
3	**ATSA VSA**	ATSA	**ED-160 [7]**
4	**ATSA AIRB**	ATSA	**ED-164 [8]**

Table 1. Prototype Iteration One supported ADS-B application

The ADS-B-NRA application is part of the baseline for this project and ADS-B-APT will be covered in iteration 2.

6.0 Airborne Surveillance ATSA ADS-B Applications

The scope of the WP15.4.5b Prototype First Iteration task is to implement enhancements into the ADS-B ground system comprising enhancements to the ADS-B ground station to incorporate new functions to improve the integrity of the supplied data [9], modifications to the ASTERIX CAT 21 and CAT 23 to carry the new integrity flags and data items [10] and enhancements to the ARTAS Surveillance Data Processing Distribution system to process the modified ADS-B data within the Multi-Sensor Tracker (MST) function [11]. It is therefore assessed that all of the 15.4.5b introduced enhancements were located within the Ground Domain of the RFG Generic Surveillance Functional Architecture (Figure 2).

Inspection of the published EUROCAE standards for the ATSA applications supported by the 15.4.5b Prototype First Iteration revealed the following conclusions regarding the Ground Domain [6]-[8]:

- The ATSA-ITP and ATSA-AIRB applications Operational Service Environment Definition (OSED) stated that all of the required ADS-B functions are located within the Aircraft Transfer and Receive Domains and the ADS-B functions contained within the Ground Domain are not required for or pertinent to the ATSA applications [6], [8]. The RFG ADS-B Surveillance Functional Architecture diagrams showed the Ground Domain as out of scope for the ATSA applications. In addition, the ADS-B AIR-B OSED stated that no system capabilities were imposed on the Ground Domain as a result of the AIR-B ADS-B application.
- The ATSA-VSA application OSED stated again that all of the required ADS-B functions to support the VSA application were located within the Aircraft domains, as witnessed by the RFG ADS-B Surveillance Functional Architecture diagram within ED-160 [7]. However, it did state that there is a requirement for the Ground Domain to provide a periodic update of the aircraft identification information using radar to undertake the VSA Advanced Procedure. ATSA-VSA assumes however the presence of a radar (independent from ADS-B) and would this not be case at implementation level, then a specific safety assessment should be undertaken (e.g. at local level) to cover the possible case of common mode of failure between airborne and ground surveillance. Further information on the ATSA-VSA application can be found within the EUROCONTROL PSC ADS-B VSA document [21].
- It should be noted that the use of ADS-B data within the Ground Domain is not a requirement within the ATSA-VSA application and hence it is assessed that no additional Safety Requirements are placed on the enhanced ADS-B Ground System as a result of supporting the ATSA-VSA application.
- Within the INTEROP assessments it was declared that the applications have no ADS-B aspects to them and hence no INTEROP requirements are levied against the enhanced ADS-B Ground System in the Ground Domain within the assessed ATSA applications.
- The ATSA-ITP and ATSA-AIRB application Operational Performance Assessments declared that they did not impose any performance requirements on the interface between the Aircraft Domain and Ground Domain, as the application was performed in Procedural Airspace where radar coverage is not expected.
- The Operational Safety Assessment conducted within the ITP, VSA and AIR-B ATSA standards identified no Operational Hazards and Internal Mitigation Means against the Ground Domain functions, only against those ADS-B functions located within the Aircraft Domains.

Based on the assessment of the ATSA SPR standards it is therefore concluded that for WP15.4.5b Prototype First Iteration, all of the safety requirements placed on the ADS-B Surveillance Functional Architecture Ground Domain are located within the ADS-B GS RAD application.

7.0 Ground Surveillance ADS-B RAD application

7.1 Introduction

The SPR standard ED-161 was developed to document the SPR and INTEROP requirements for the implementation of the Ground Surveillance ADS-B application, 'Enhanced Air Traffic Services in Radar-Controlled Areas using ADS-B surveillance' or ADS-B RAD. It was defined to support and in some cases enhance ATS service provision though the addition of ADS-B coverage in areas where radar surveillance current exists [3].

The ADS-B RAD application was specified to apply to En Route and Terminal airspace, in airspace classes A to D. It was specified to support the following ICAO Air Traffic Services; Air Traffic Control Service (i.e., Area Control Service and Approach Control Service), Flight Information Service, Alerting Service and Air Traffic Advisory Service [3].

Enhancements to the delivered ATS services through the implementation of ADS-B service in addition to the existing radar ones would be through an overall improvement to the quality of the surveillance information and this could deliver ATS operational benefits through the reduction in applied horizontal position separation standards within the RAD airspace in-question.

ED-161 featured an OSED, an SPR assessment comprising an OPA and OSA and INTEROP assessment in accordance with the standard ED-78A process. In addition, it also featured an Surveillance Separation Error (SSE) assessment in support of the performed OPA and OSA processes, as shown in Figure 5 [3].

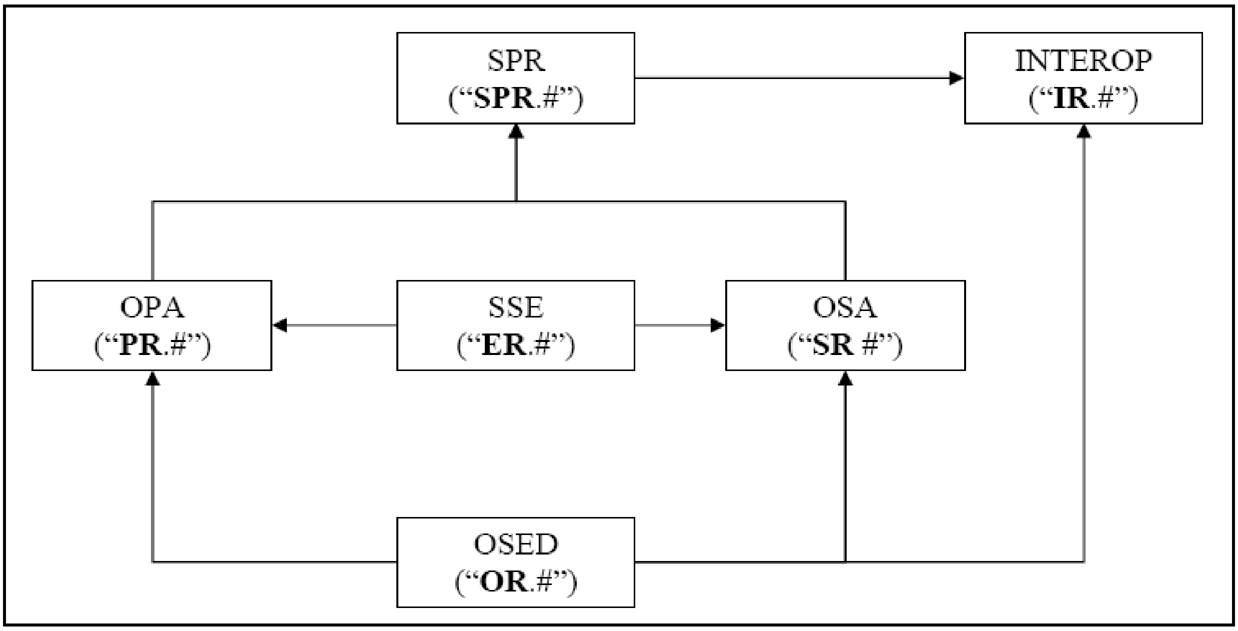

Figure 5. ED-161 SPR and INTEROP assessment showing additional SSE analysis

The OSED, OPA, OSA and SSE assessments and derived requirements set are contained within separate annexes in ED-161. After completion of the assessments, the resultant requirements sets are combined into an consolidated SPR chapter within ED-161 termed Chapter 3. Interoperability requirements are presented within ED-161 Chapter 4 [3].

7.2 ADS-B RAD OSED

7.2.1 ADS-B RAD Environment Scenarios

The ADS-B RAD OSED defined a set of Operational Environments comprising airspace type, traffic density and applied separation minima and Surveillance system deployment scenarios, which featured the ADS-B layer combined with a single layer of radar surveillance [3]. These two elements were combined into ADS-B RAD Environment Scenarios (ES) and are described within Table 2 [13]:

	ATS surveillance system supporting ADS-B-RAD system	Typical Operational Environment
RAD-1	Single Primary Surveillance Radar (***PSR***) with ***ADS-B*** surveillance.	*ENVT-1:* medium traffic density in TMA airspace, applying 3NM separation minima
RAD-2a	Single mono-pulse Secondary Surveillance Radar (***SSR***) with ***ADS-B*** surveillance.	*ENVT-2*: high traffic density in En-route airspace, applying 5NM separation minima
RAD-2b	Single ***Mode-S*** radar with ***ADS-B*** surveillance.	*ENVT-2*: high traffic density in En-route airspace, applying 5NM separation minima
RAD-3	Single Primary Surveillance Radar (***PSR***) with a collocated single Secondary Surveillance Radar ***(SSR)*** together with ***ADS-B*** surveillance.	*ENVT-3*: high traffic density in TMA airspace, applying: • 3NM separation minima in the wide area • 2.5NM separation minima for succeeding aircraft on same final • 2 NM separation minima for succeeding aircraft on adjacent ILS/MLS

Table 2. ADS-B RAD Environment Scenarios

The ADS-B RAD ES were derived through comparison with 'Reference' radar scenarios, which replicated the composition of the above scenarios but featured two layers of radar surveillance. In the reference radar scenarios, the ADS-B surveillance layer was replaced by a layer of SSR in RAD-1, RAD-2a and RAD-3 and a layer of Mode S SSR within RAD 2b [13].

It should be noted that the scenarios are defined within ED-161 were declared as minimum representative surveillance scenarios, comprising only a single layer of radar combined with ADS-B. It stated that more complicated scenarios involving ADS-B in combination with multiple layers of radar surveillance, newer forms of surveillance such as Wide Area Multilateration (WAM) systems and advanced multi-sensor processing and distribution systems were outside of the scope of the performed OPA and OSA analysis [3].

This conclusion was also reached when assessing the direct applicability of ED-161 to a surveillance system deployment scenario featuring the 15.4.5 Enhanced ADS-B Ground System, as described in Section 8.

7.2.2 ADS-B RAD Surveillance Functional Model

Inspection of the ED-161 OSED revealed that against the generic RFG ADS-B Surveillance Functional Architecture (Figure 2) all Aircraft and Ground Domains were declared as relevant to the ADS-B RAD application [3].

The RAD SPR document modified the ADS-B RFG generic Surveillance Functional Model (Figure 2) into the ADS-B application RAD functional model shown in Figure 6. The implemented changes modelled the required ground based functions within the ADS-B combined with radar surveillance scenarios and radar reference scenarios introduced within the ADS-B RAD OSED [3].

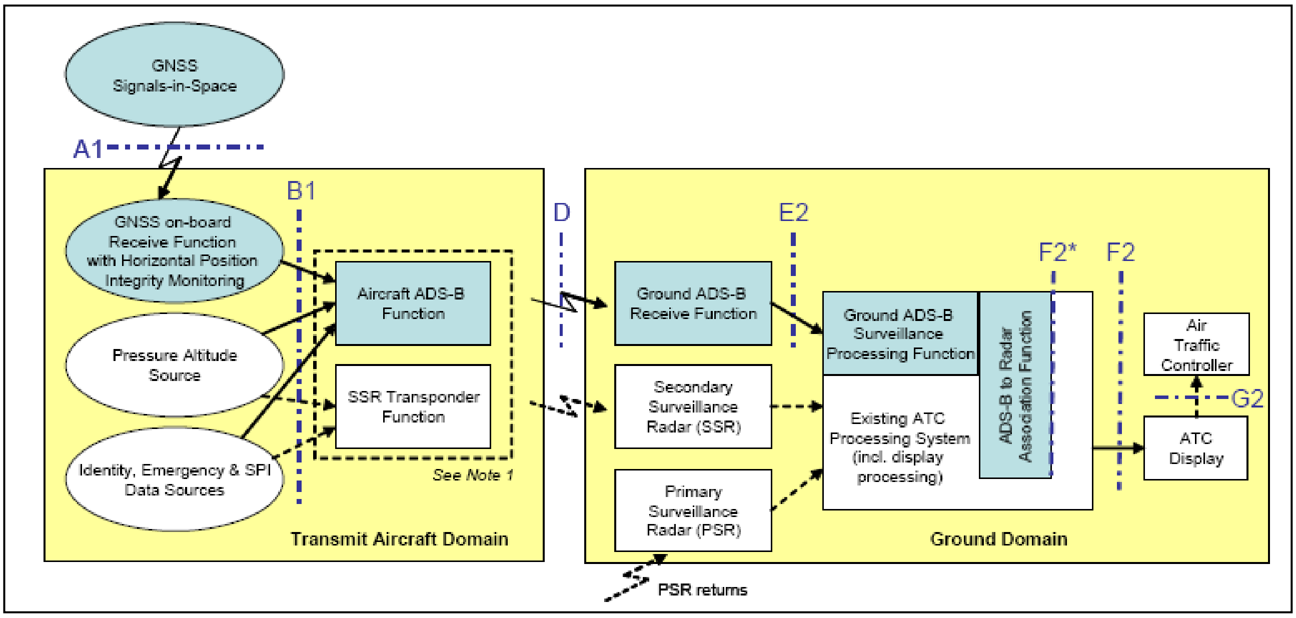

Figure 6. ADS-B RAD application Surveillance Functional Model

The ADS-B RAD Functional Model expanded the level of detail within Transmit Aircraft Domain for the data sources used to input data into the RFG 'ADS-B Transmit Function' (RAD model Aircraft ADS-B Function) and RFG 'SSR Interrogation Reply' function (RAD model SSR Transponder Function). This expansion was to reinforce the commonality of the aircraft identity and height data output on the ADS-B and SSR transmit functions between interfaces A1 and D [3].

Within the Ground Domain, the RFG 'ADS-B Receive Subsystem and other surveillance inputs' function was separated into 'PSR Receive', 'SSR Receive' and 'Ground ADS-B Receive' functions (interface D-E2). The RFG 'ATC processing system' function was divided into two processing paths, a ADS-B data processing path (interface E2-F2) and radar data processing path. [3].

7.3 Surveillance Separation Error analysis

In support of both the OPA and OSA, a Surveillance Separation Error (SSE) analysis has been performed (see Ref 3, Annex D). In particular, with respect to the OPA, the SSE determines the horizontal position containment bound (Navigation Integrity Category, or NIC) per the various separation minima scenarios considered in the ADS-B-RAD standard document. In addition, the SSE provides a key input into the establishment of the OSA event trees (through the so-called Probability of effect (Pe) probabilities). The relationship between the SSE and OPA/OSA is depicted in Figure 5.[3].

7.4 ADS-B RAD Operational Performance Assessment

The ED-161 Operation Performance Assessment (OPA) evaluated the ADS-B RAD Performance Requirements in the nominal or no-fault situation, using the Operational Requirements and Assumptions defined within the OSED. It concentrated on the ATS separation task, deeming this the most demanding ICAO Air Traffic Control application performed within the mixed radar and ADS-B data environment [3].

The Operational Performance Assessment (OPA) compares key attributes of radar with key attributes of ADS-B surveillance data. The premise of the analysis is that if ADS-B data is of equal or superior quality to radar data, then ADS-B data can be used in the same manner as radar data is today. The OPA analysis represented the ‘success’ case for the performed safety assessment and for further information the reader is referred to the EUROCONTROL PSC ADS-B RAD document [13].

7.5 ADS-B RAD Operational Safety Assessment

ED-161 Operational Safety Assessment (OSA) followed the normal ED-78A format, featuring an Operational Hazard Assessment (OHA) and an Allocation of Safety Objectives and Requirements (ASOR) activity [4]. An overview of the OSA process, termed the 'bowtie' model is shown in Figure 7, complete with commonly used OSA terms [3]:

BC	Basic Cause	AE	Abnormal Event
IMM	Internal Mitigation Means	SO	Safety Objective
OH	Operational Hazard	EMM	External Mitigation Means
OE	Operational Effect	ST	Safety Target
SR	Safety Requirements	EC	Environment Conditions

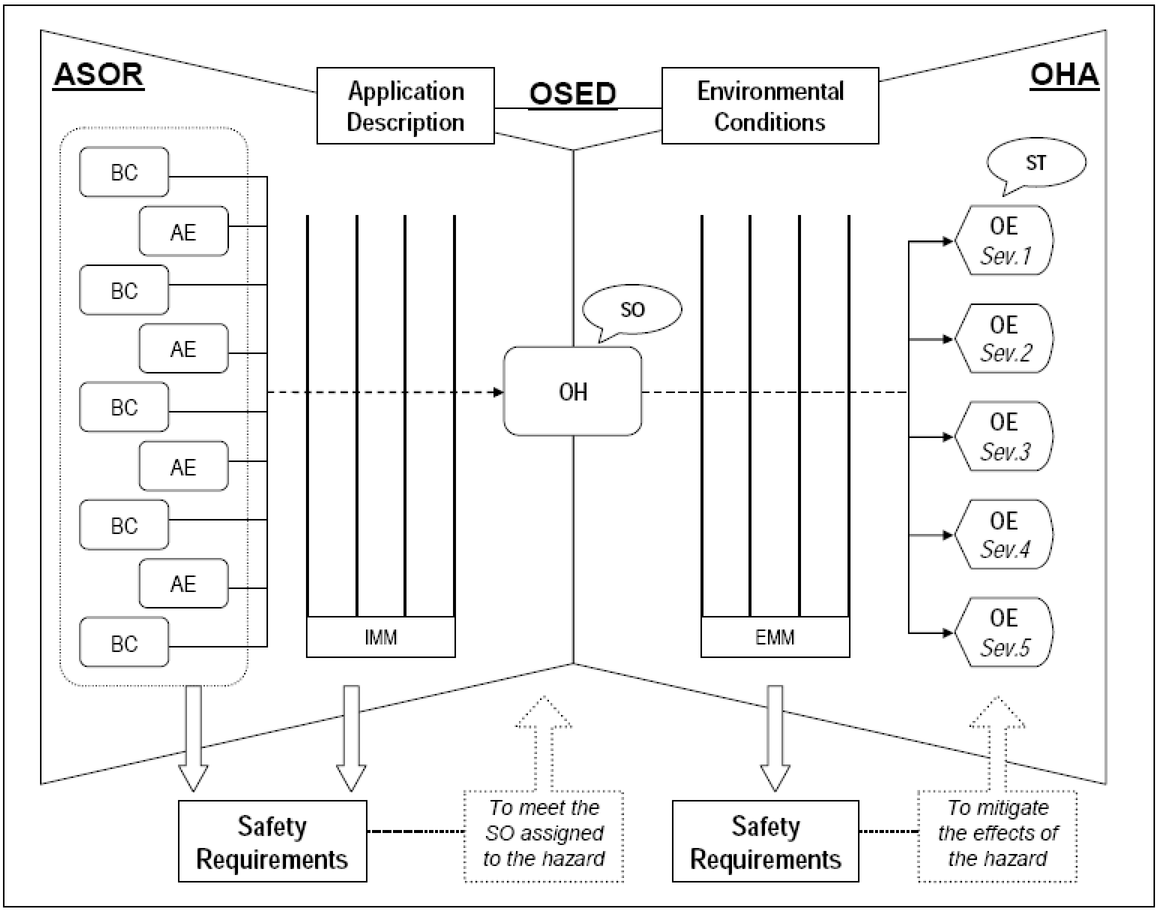

Figure 7. OSA Process diagram

The first step in the OSA process is to define the Operational Hazard set within the OHA, followed by the use of event trees to derive Safety Targets and hence Safety Objectives for the assessed ATM system using calculated Severity and Probability of effect (Pe) values for each Operational Hazard. External Mitigation Means (EMM) which act to lower the Severity and Pe values for the assessed OH set are used to define Safety Requirements on the ATM system.

The ASOR process then takes the defined Safety Objectives and apportions them to Severity class of OH and hence derives Safety Requirements (SR) on the systematic elements of the application to meet the defined Safety Objectives. Internal Mitigation Means (IMM) which act to enable the ATM system to meet the required SO are also used to define Safety Requirements.

7.5.1 Operational Hazard Assessment

The ED-78A OHA process is a four step process, shown in Figure 8 and in the right hand half of Figure 7 [3]:

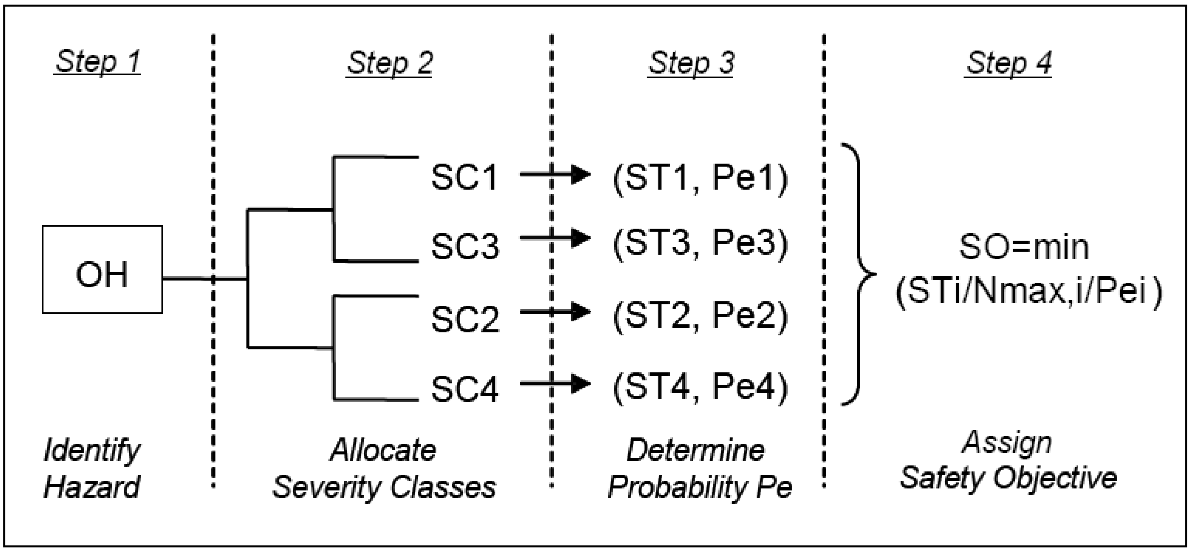

Figure 8. Operational Hazard Assessment – OSA process steps 1-4

- OSA Step 1 is to identify the Operational Hazard set.
- OSA Step 2 allocates a ESARR 4 defined Severity Class against each identified OH through the use of an event tree.
- OSA Step 3 determines the Probability of effect value against each OH through assessment of each event tree branch and
- OSA Step 4 allocates a Safety Objective against each OH, using the most stringent value assessed from the Safety Target and Pe for each event tree scenario.

7.5.1.1 OSA Step 1 - Operational Hazards identification

Step 1 is to define the Operational Hazards (OH) for the RAD application through ATS operational input from ATC experts, Safety SME's and pilots. All OH conditions identified against the ADS-B RAD application either concerned i) the loss of ADS-B data or ii) the provision of credibly corrupt ADS-B data to the ATCO.

The RAD application OH list is reproduced in Table 3 [3], [13]:

Hazard Id	Hazard Description: Single Aircraft event
OH01	Sudden and Unexpected Loss of ADS-B Position Information for a *Single* Aircraft
OH03	Loss of All ADS-B Data for a *Single* Aircraft
OH05	Incorrect Position Information for a *Single* Aircraft – divided into three sub-cases:

Hazard Id	Hazard Description: Multiple Aircraft event
OH02	Sudden and Unexpected Loss of ADS-B Position Information for *Multiple* Aircraft
OH04	Loss of All ADS-B Data for *Multiple* Aircraft
OH06	Incorrect Position Information for *Multiple* Aircraft – divided into three sub-cases:

Hazard Id	Hazard Description: Single Aircraft event	Hazard Id	Hazard Description: Multiple Aircraft event
OH05-1	*Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring for a Single Aircraft*	*OH06-1*	*Horizontal position error resulting from a GNSS position source error not detected by the aircraft integrity monitoring for Multiple Aircraft*
OH05-2	*Horizontal position error resulting from a sustained credible corruption of the position information for a* Single Aircraft	*OH06-2*	*Horizontal position error resulting from a sustained credible corruption of the position information for* Multiple *Aircraft*
OH05-3	*Horizontal position error resulting from a sustained credible corruption of the quality indicator for a* Single Aircraft	*OH06-3*	*Horizontal position error resulting from a sustained credible corruption of the quality indicator for* Multiple *Aircraft*
OH07	Loss of Emergency Mode after Selected by Flight Crew		
OH08	Incorrect but Plausible Emergency Mode		
OH09	Two 'Dispersed' Position Symbols for the *Same* Aircraft	**OH10**	*Multiple* 'Dispersed' Position Symbols
OH11	Incorrect Level Information for a *Single* Aircraft	**OH12**	Incorrect Level Information for Multiple Aircraft
OH13	Loss of Level Information for *Single* Aircraft	**OH14**	Loss of Level Information for *Multiple* Aircraft
OH15	Incorrect Identity data for a *Single* Aircraft	**OH16**	Incorrect Identity data for *Multiple* Aircraft – divided into two sub cases:
		OH16-1	*Incorrect ID resulting from a sustained credible corruption of ID for* Multiple *Aircraft*
		OH16-2	*Transposition of IDs between at least two aircraft (swap ID)*
OH17	Loss of Identity data for a *Single* Aircraft	**OH18**	Loss of Identity data for *Multiple* Aircraft
OH19	*Single* False Target	**OH20**	*Multiple* False Targets

Table 3. ADS-B RAD application defined Operational Hazards

In conjunction with the OH determination, a set of Environment Conditions (EC) were specified regarding the characteristics of operating environment in which the RAD application is expected to deployed within [3]. Inspection of the ED-161 revealed that the listed EC contained the ATC related assumptions with regards to a particular OH and these constituted the basic assessment assumptions, as the generated results where directly dependant on them.
It was found that only 7 from the 20 ADS-D RAD application OHs had one or more EC's against them and it was further stated that each EC may increase or reduced the severity of the identified operational hazard condition, dependant on the environment characteristics i.e. high density vs. low density traffic, Enroute or TMA airspace, etc [3].

7.5.1.2 OSA Step 2 – Hazard assessment and Severity Classification

The OHA process now takes each Operational Hazard, completed with defined Environment Conditions and identifies the potential operational effects of the hazard occurring on ATS provision. The Step 2 assessment is performed by safety experts, with operational ATC input from Step 1.

The assessment process is captured as an event tree for each assessed OH [13]. The event tree represents a logical model that identifies and quantities all possible outcomes following the occurrence of the hazard condition (initiating event). Each branch of the event tree describes an EC or EMM related to the OH and is termed a 'barrier' to the hazard occurrence. The event tree describes the 'success' and 'failure' probability of each identified barrier. At the end of each branch the effects of each hazards are assessed, giving it corresponding Severity Class [13].

External Mitigation Means (EMM) may be identified against each OH, which are mitigation means between the hazard and its final effect. EMM can help to reduce the impact of the hazard once it has occurred. Where an EMM acts as a barrier within the event tree assessment, a Safety Requirement is raised to capture the required performance of the mitigation means [3].

The Severity of the hazard is graded into different classes depending on the effect to ATC service provision, Flight Crew and the aircraft hull. EASARR 4 defines Severity Classes using the Table 4 indices [14]:

Severity	Effect on Operations	Effects on ATC operations
1	Accidents	No independent source of ATC or aircrew recovery mechanism One or more catastrophic accidents, hull loss, fatalities
2	Serious Incidents	Large reduction in separation without crew or ATC fully controlling the situation Significant manoeuvre required to avoid aircraft or terrain collision
3	Major Incidents	Large reduction in separation minima, with crew or ATC fully controlling the situation Minor reduction in separation without crew or ATC fully controlling the situation
4	Significant Incidents	Slight reduction in ATC safety margins within full control Increased ATC or crew work load
5	No safety effect	No hazardous condition

Table 4. ESARR 4 Hazard Severity classification matrix

Severity 1 is the most severe to ATC operations resulting in hull loss and fatalities, decreasing in the severity of effect to level 5 which represents the no impact to ATC operations.

7.5.1.3 OSA Step 3 –Probability of effect and Safety Target determination

The 'Probability of effect' or 'Pe' value for each assessed OH expresses the probability of the OH occurrence leads to an Operational Effect (OE) for the hazard, having a Severity Class evaluated in Step 2 [15]. 'Pe' is calculated based on the success/failure probability of each identified event barrier and hence gives a measure of the effectiveness of the barriers to the effect of the hazard occurring [3], [15]:

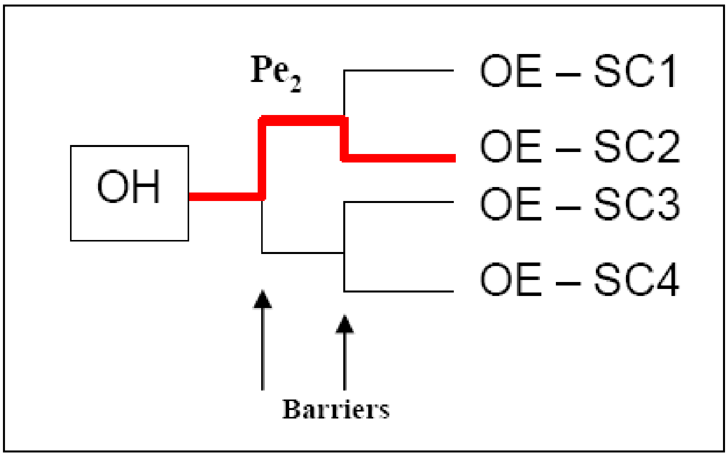

Figure 9. Pe determination process for each OE against a particular OH

Each branch of the event tree contributes a 'Pe' value against each assessed OH to OE-SC_j combination within the hazard, where 'j' refers to the index of the Severity Class assigned to each event tree branch.

7.5.1.4 OSA Step 4 – Safety Objective Assignment

Safety Targets for each OH Severity class are determined using a Risk Classification Scheme, proposed within ESARR 4 for Severity Class 1 incidents [14] and further developed within ED-125 for Severity classes 2, 3 and 4 [15]. Severity Class 5 were not assessed, as they had no ATC impact.

Safety Targets are defined within ED-125 as

- Safety Target or ST_j specifies the overall maximum frequency of occurrence of effects of any type having a given Severity Class j (SC_j) whatever the ATM cause.

ESARR 4 proposed an overall Safety Target for each Severity class (Figure 7), which was applied for all operational hazards appearing within that class [14]. ED-125 expanded this concept into three tiered levels for European ATM Safety Targets [15];

i) ECAC wide Safety Target,

ii) National Regulator Safety Target,

iii) ATM Service Provider or ATMSP Safety Target.

ST values for each Severity Class (1-4) were linked through Ambition Factors, which acted to reduce the higher level Safety Target to the more stringent value for the lower level through the use of equations (1) and (2):

$$\frac{\text{ECAC level } ST_j}{AF_1} = \text{National Reg } ST_j \qquad (1)$$

$$\frac{\text{National Regulator } ST_j}{AF_2} = \text{ATMSP } ST_j \qquad (2)$$

where 'j' is the index of the Severity Class i.e. 1-4 [15]

ESARR 4 and ED-125 proposed the set of ECAC, National Regulator and ATMSP Safety Targets and Ambition Factors shown in Table 5:

Safety Target	ECAC level ST_j (per flight hr)	Minimum AF_1	Maximum National Regulator ST_j (per flight hr)	AF_2	Maximum ATMSP ST_i (per flight hr)
ST_1	1.55E-08 [14]	1.55	1E-08	**10**	**1e-09**
ST_2	1E-05 [15]	1	1E-05	**10**	**1e-06**
ST_3	1E-04 [15]	1	1E-04	**10**	**1e-05**
ST_4	1E-02 [15]	1	1E-02	**10**	**1e-03**

Table 5. ED-125 Safety Targets for Severity Classes 1-4 hazards

The Ambition Factors were imposed to act to 'future proof' the implemented ATS system against changes the air traffic management environment e.g. traffic density increases, airspace design modifications, capacity changes, etc [13].

The final step of the Safety Target derivation was to apportion each overall Severity Class ST value to a Safety Target per Severity Class per Operational Hazard, using an assumed Operational Hazard occurrence distribution for Severity Class 1 to 4. The ADS-B RAD OHA used an ED-125 Model 3 distribution featuring 125 hazards, split into [15];

- Nmax = 2 for Severity Class 1 hazards,
- Nmax = 25 for Severity Class 2 hazards,
- Nmax = 25 for Severity Class 3 hazards and
- Nmax = 73 for Severity Class 4 hazard.

The ADS-B RAD assumed Severity Class Operational Hazard distribution modified the overall ATMSP ST values per Severity Class given in Table 5 to give ST values per OH in each Severity Class shown in Table 6, through the use of equation (3) [13]:

$$\frac{\text{ATMSP } ST_j}{\text{Nmax}} = \text{ST per RAD OH or } ST_{RADj} \qquad (3)$$

The new values for Safety Targets per Operational Hazard for each Severity Class or ST_{RADj} now are given by Table 6:

Safety Target	ATMSP ST (per flight hr)	Nmax	ST per RAD OH or ST_{RADi} (per flight hr)
ST_1	**1e-09**	2	5E-10
ST_2	**1e-06**	25	4E-08
ST_3	**1e-05**	25	4E-07
ST_4	**1e-03**	73	1.4E-05

Table 6. ADS-B RAD ST values per individual OH

The final step of the Operational Hazard Assessment is the calculation of the Safety Objective per OH per Severity Class SO_j, as shown in Figure 8. This was achieved within the ED-161 through the use of equation (4) [3]:

$$\text{Safety Objective} \quad SO_j = \frac{ST_{RADj}}{Pe_j} \qquad (4)$$

Where 'j' is the index of the Severity Class.

The ADS-B-RAD PSC provides a consolidated view of ST on a "per severity class" instead of a "per individual hazard" (as done on the ADS-B-RAD standard). This is simply a different view and did not affect the requirements derivation. For this purpose the number of individual hazards, per specific environment, is identified (see table 7 extracted from PSC annex F) and use in the consolidation into "per severity class" (see table 8 below extracted from the PSC eannex F). It should be noted that in addition to the per flight hour values, sector hour values have been presented as well, using an assumed density of aircraft movements per hour expected within a single ATC sector for the different operating environments. [13].

Severity	Nmax	N_{RADi}		
		RAD-1	RAD-2	RAD-3
1	2	3	3	3
2	25	6	4	4
3	25	5	7	7
4	73	7	7	8
Total	125	21	21	22

Table 7. PSC ADS-B Modelled Hazard Distribution per Severity Class

Severity	ST per OH	ST_{RADi}		
		RAD-1	RAD-2	RAD-3
1	5E-10	1.5E-09	1.5E-09	1.5E-09
2	4E-08	2.4E-07	1.6E-07	1.6E-07
3	4E-07	2.0E-06	2.8E-06	2.8E-06
4	1.4E-05	9.8E-05	9.8E-05	1.1E-04

Table 8. ST_{RADi} values for RAD-1, RAD-2 and RAD-3 scenarios

To determine the Safety Objective per Operational Hazard in each SC therefore requires each ST_{RADi} value to be modified through the use of equation (5) [13]:

$$\text{Safety Objective} \quad SO_i = \frac{ST_{RADi}}{Pe_j \; N_{RADi}} \qquad (5)$$

Therefore, the Safety Objectives per OH derived using the ADS-B RAD OSA method and PSC ADS-B RAD method are identical in value.

7.5.2 Allocation of Safety Objectives and Requirements

Allocation of Safety Objectives and Requirements activity apportions the Safety Objective evaluated for every OH to basic causes/abnormal events which trigger each Operational Hazard. After apportionment, these triggering conditions in-conjunction with the application Environment Conditions, are incorporated into failure probability fault trees [3], [4].

Fault trees logically link failure probabilities together to determine if the ATM system design meets the overall Safety Objective for each identified OH. If the ATM system design is shown to meet the Safety Objective then the fault tree gates are used to derive Safety Requirements for the ATM system design. If the SO is not met, then additional Internal Mitigation Means (IMM) can be incorporated into the ATM system design and hence the fault tree model for each OH until the SO is satisfied. The implemented IMM therefore generate Safety Requirements on the ATM system design.

The ASOR process step sequence is shown schematically below and also in the left hand side of Figure 7:

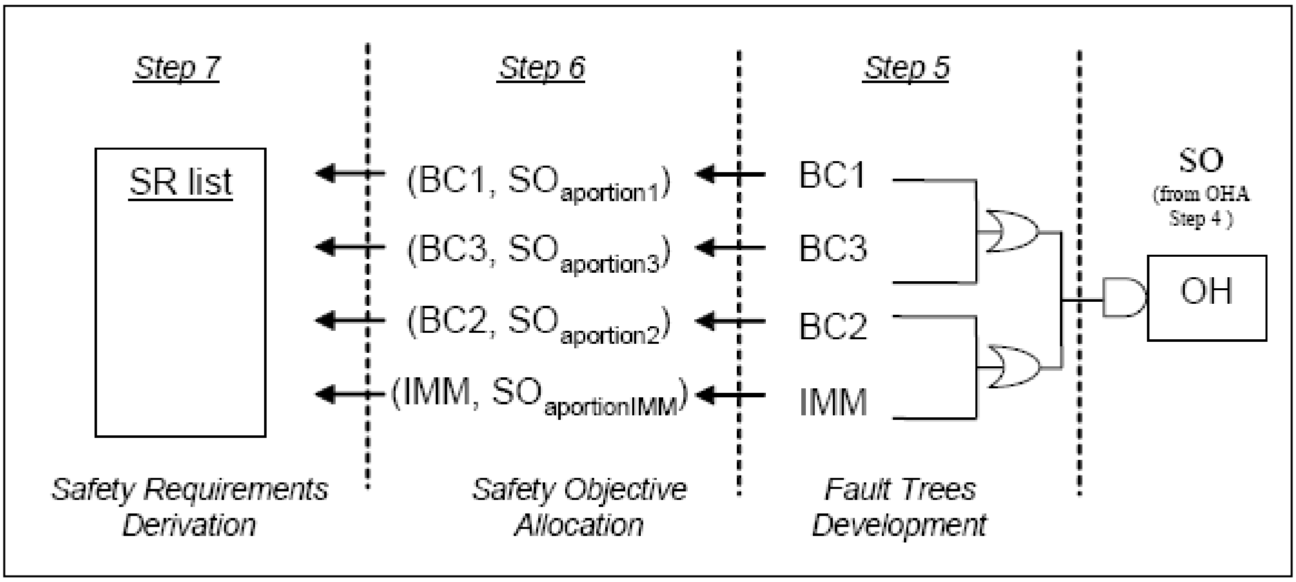

Figure 10. Allocation Safety Objective and Requirements – OSA steps 5-7

7.5.2.1 OSA Step 5 - Fault Tree Development

The ASOR activity develops a fault tree for each OH. The fault tree models the basic causes of the modelled hazard through Basic Events (BE), Environment Conditions (EC) and Internal Mitigation Means (IMM), which through linked failures lead to the hazard occurring [3]:

- Basic Events (BE) are the combination of Basic Causes and Abnormal Events shown in the left hand side of Figure 7 of the hazard condition. They are probability of failure values for the assessed conditions. Examples of BE's from ADS-B RAD OSA OH-01 includes loss or corruption of GNSS signals in the Aircraft Transmit Domain causing horizontal position errors within the ADS-B messages (failure probability of 1E-5) and loss or corruption of the ADS-B messages within the Ground Domain ADS-B message reception function (failure probability of 1.70E-6).

- Environment Conditions (EC) are characteristics of the target application operating environment. An example EC extracted from the ADS-B RAD OSA OH-01 is that corruption in ADS-B position data causes a aircraft reported position error > 10NM from the true aircraft position. This condition is detected by the Ground Domain in 99.99% of all cases and hence the failure probability is defined as 9.99E-1 to 2 significant figures.

- Internal Mitigation Means are mitigations present within the boundaries of the application functional model which help the achievement of the safety objective assigned to the hazard. IMM's can be integrated within the fault tree so that they must fail for the hazard condition to occur. An example of IMM extracted from ADS-B RAD OSA OH-01 was that the ground system would identify if the ADS-B position was greater than 10NM from its true position in >99% of all cases. Therefore, the failure probability for this IMM was set to 9.9E-1.

A fault tree decomposes an Operational Hazard into a set of linked failures contained within a fault tree branch which must occur for the hazard to happen. The starting event for each fault tree branch can be a BE, IMM or EC, shown by the Basic Causes box in Figure 11. The failure cases are represented by probability values for their occurrence and these initial probabilities are derived from OSA assumptions assessed to be relevant to the particular hazard. The top level OH probability is used to determine whether the apportioned safety objective can be met for the detected and undetected case of each OH [3].

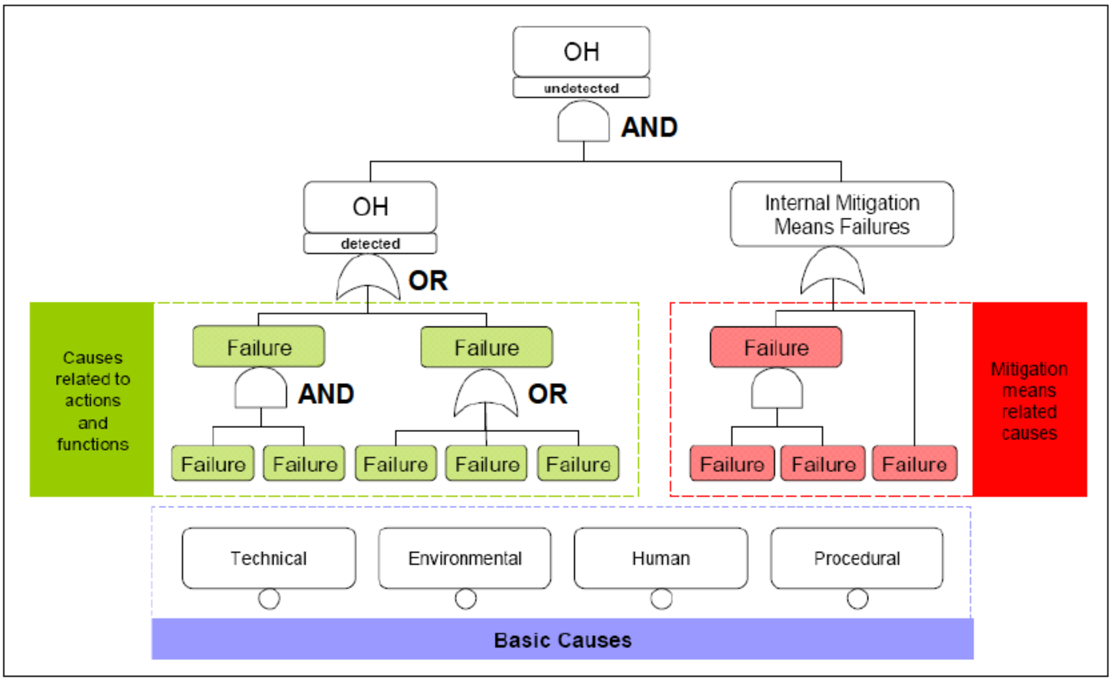

Figure 11. ASOR process generic Operational Hazard fault tree

Failure conditions within the fault tree are linked via 'AND' gates or 'OR' gates. Where a failure condition is represented by an AND relationship, the lower level input failure probabilities are multiplied together to achieve the upper level value and hence all must occur for the hazard condition to be present. Where a failure condition is represented by an OR relationship, the lower level failure probabilities are summed together to achieve the higher level failure probability. In this case, any one of the input failures can cause the hazard to occur [3].

7.5.2.2 OSA Step 6 - Safety Objective Allocation

The Safety Objective Allocation step within the OSA process is performed to demonstrate that the proposed functional architecture, as captured within the fault trees, meets the safety objectives identified for each hazard [3].

Each OH has a likelihood of occurrence probability captured within the top level of the fault tree, linked through the branches of the fault tree to the failure rates of the identified Basic Events and Internal Mitigation Means. This likelihood of occurrence probability is compared against the hazard's allocated safety objectives and if it is lower than the most stringent SO then the current functional architecture can be declared to met the safety objectives [3].

If the likelihood value is greater than any of the safety objectives then additional fault tree mitigation means (IMM) or event tree barriers (EMM) may need to be identified to effectively mitigate the hazard to a tolerably safe level. These additional mitigation means would need to be incorporated within the event and fault trees and hence would act to increase the number of Safety Requirements raised against the aircraft or ground functional model elements [3].

7.5.2.3 OSA Step 7 – Safety Requirements Derivation

The final step of the OSA process is to derive Safety Requirements from the fault tree analysis. Each basic cause is assessed and the relevant OSA assumptions used to define a set of corresponding Safety Requirements on the application and the surveillance system elements under assessment. Certain fault tree gates can also be used to define system Safety Requirements, which link combinations of basic causes together into a single requirement [3].

Within the ADS-B RAD OSA, Safety Requirements were generated against the assessed ADS-B system and reference radar scenarios [3].

8.0 Applicability of the ADS-B RAD SPR standard to the 15.4.5 Enhanced ADS-B Ground System

8.1 Enhanced ADS-B Ground System OSED

8.1.1 Enhanced ADS-B Ground System Environment Scenarios

The ADS-B RAD OSED defined candidate surveillance Environment Scenarios for the OPA and OSA assessments, based upon one layer of radar surveillance and one layer of ADS-B surveillance. The ADS-B layer provided the prime means of surveillance, with the radar layer acting as the backup surveillance service during loss or degradation of the ADS-B service [3].

This document proposes a new surveillance Environment Scenario set, incorporating the WP15.4.5 enhanced ADS-B ground system as an element. WP15.4.5b will develop prototypes within the SESAR Development phase over the timescale 2011-2014 [5]. Given this timeframe and that current operational deployment of Mode S SSR systems within core Europe is highly advanced, it is considered that conventional SSR systems can be classified as legacy surveillance equipment and hence not considered within the majority of the considered Environment Scenarios. However, certain European ANSP's may continue to operate legacy SSR assets for economic reasons until their end of life and hence these systems are covered under the eRAD-2a and eRAD-5a ES definitions.

In common with the ADS-B RAD approach it is assumed that the prime means of ATS surveillance service provision is via the ADS-B service, with either the PSR/SSR/Mode S SSR/combined PSR-Mode S radar service or WAM service acting as the backup surveillance source.

8.1.1.1 Full 15.4.5 security benefits deployment scenarios

The enhanced ADS-B ground system features the capability to accept Wide Area Multilateration inputs into both the enhanced ADS-B groundstation and the enhanced SDPD multi-sensor tracker, to deliver ADS-B data integrity and security enhancements [5]. Therefore, to develop the full benefits from the enhanced ADS-B ground system the dependant cooperative surveillance ADS-B system must be deployed in combination with an independent cooperative surveillance WAM system.

The combined WAM and ADS-B deployments, in-conjunction with reference radar systems, lead to Environment Scenarios eRAD-1 to eRAD-3 within Table 9, with the operating environments taken directly from the ADS-B RAD OSED [3].

ES	ATS surveillance system components	Operating Environment	Reference ADS-B RAD ES
eRAD-1	Enhanced ADS-B ground system, WAM and single layer of PSR	Medium density TMA; 3NM separation	RAD-1
eRAD-2a	Enhanced ADS-B ground system and single layer of WAM and/or SSR	High density Enroute; 5NM separation	RAD-2a
eRAD-2b	Enhanced ADS-B ground system and single layer of WAM and/or Mode S SSR	High density Enroute; 5NM separation	RAD-2b
eRAD-3	Enhanced ADS-B ground system, WAM and single PSR and co-mounted Mode S SSR	High Density TMA: 3NM separation Approach: 2.5NM and 2NM separation	RAD-3

Table 9. ADS-B Environment Scenarios incorporating the full 15.4.5 security benefits

8.1.1.2 Subset 15.4.5 security benefits deployment scenarios

The enhanced ADS-B ground system can be deployed as an ADS-B only system, abet only realising a sub-set of the security enhancements [5]. The enhanced ADS-B GS plus radar ES realise the Environment Scenarios eRAD-4 to eRAD-6 contained within Table 10:

ES	ATS surveillance system components	Operating Environment	Reference ADS-B RAD ES
eRAD-4	Enhanced ADS-B ground system, and single layer of PSR	Medium density TMA; 3NM separation service	RAD-1
eRAD-5a	Enhanced ADS-B ground system and single layer of SSR	High density Enroute; 5NM separation service	RAD-2A
eRAD-5b	Enhanced ADS-B ground system and single layer of Mode S SSR	High density Enroute; 5NM separation service	RAD-2b
eRAD-6	Enhanced ADS-B ground system, and single combined PSR-Mode S SSR	High Density TMA and Approach; 3, 2.5, 2NM separation service	RAD-3

Table 10. ADS-B Environment Scenarios incorporating a subset of 15.4.5 security benefits

It should be noted that the operating environments are directly taken from the ADS-B RAD application OSED.

8.1.2 Enhanced ADS-B Ground System Surveillance Functional Model and Architectural Implications

The RFG generic Surveillance Functional Model was tailored to the specifics of the ADS-B RAD application, as described within Section 5.3.2.2. The RAD application defined Functional model will require further modification to incorporate the enhanced ADS-B ground system, with the proposed Enhanced ADS-B Ground System Surveillance Functional Model shown in Figure 12:

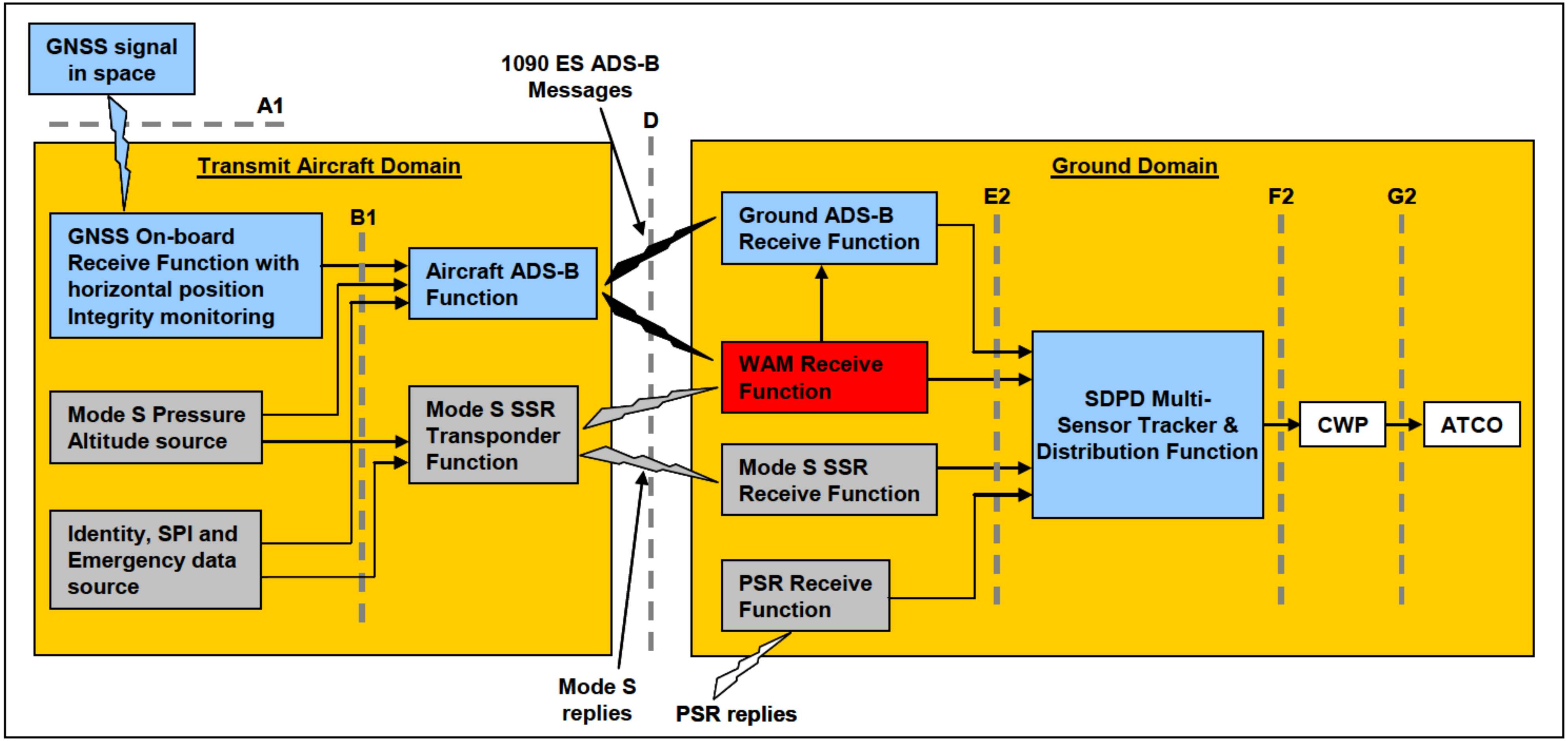

Figure 12. Enhanced ADS-B ground system Surveillance Function Model

Salient points of the 15.4.5 functional model comprise, in parallel with the approach proposed within the D18 document [16]:

- Aircraft ADS-B Function will be delivered via ADS-B_{OUT} services from Mode S Transponders compliant to DO-260B/updated version of ED102A [5].
- Ground ADS-B Receive function will be delivered via the enhanced ADS-B ground station, with optional WAM input.
    - If the ADS-B groundstation is implemented in standalone ADS-B operation then its function matches the description within the ED-161 OSA [3].
    - If the WAM ASTERIX CAT20 target reports are used to validate the decoded ADS-B data ASTERIX CAT 21 output, subject to the WAM ASTERIX CAT 19 service messages declaring the WAM system in a GO state, then the ADS-B groundstation functions in the manner described within the D05 document [9].
- The optional WAM Receive Function between the D and E2 interface. This produces ASTERIX CAT 20 target reports and CAT 19 service messages, which are input into the SPDP Multi-Sensor Tracker [11] and can be input into the ADS-B groundstation to validate the decoded ADS-B message horizontal position and identity data items [9].
- Combination of the RAD application Ground ADS-B Surveillance Processing Function, ADS-B to Radar Association Function and Existing ATC Processing System function into the enhanced Surveillance Data Processing and Distribution (SDPD) Function between the E2–F2 interfaces. The ARTAS SDPD Multi-Sensor Tracker fuses input surveillance data supplied in various ASTERIX formats from ADS-B (enhanced and non-enhanced), radar, and WAM sources into a system track for each detected aircraft. The created air situation picture is served to various end users, including CWP's and hence the controlling ATCO.
- The modification of the ATC Display to the modern Controller Working Position terminology between the F2-G2 interfaces [17].

The combination of the RAD application ADS-B processing functions into the enhanced SDPD function within the 15.4.5 ground system is further specified within the Baseline Matrix for the first iteration prototype [17].

8.1.3 Prototype First Iteration Security Enhancement Functionality

A significant number of ADS-B data information security enhancements were incorporated into WP15.4.5b Prototype First Iteration Ground System. These enhancements compromised the following list, with the test result reported to the SDPD though a validation flag having three states: VALID, NOT VALID or NOT_VALIDATED [11], [16]:

- ADS-B Ground Function Receive (ADS-B Groundstation) integration with WAM. ADS-B 2D position information validated through comparison with horizontal position reported within the WAM target report for the same aircraft.
- Angle of Arrival (AoA) measurement for the ADS-B message RF signal and comparison of the angular difference between the measured (AoA) and that calculated from the reported position decoded from the ADS-B message.
- Reported horizontal position evolution of the target position vs reported aircraft velocity check.
- Power measurement and range correlation involving the matching the decoded target position and hence range from the ADS-B groundstation and the amplitude of the received RF message
- Time of Arrival (ToA) validation of the ADS-B message transmitter involving the decoding of the same message at multiple groundstation and the use of the message ToA to validate the reported position information

Multi-sensor Tracking within the SDPD helps to the determine the validity of the reported ADS-B position and identification information through the use of other cooperative surveillance sources i.e. SSR, Mode S SSR, WAM providing target reports into common overlapping coverage volumes. The comparison process uses both the reported position and identification information from all input surveillance sources and through inspection of the validation result flags reported from the above ADS-B Ground System enhancements. These processes help to determine if the ADS-B report is genuine i.e. from real aircraft or false i.e. from a spoofing ADS-B transmitter or malfunctioning Mode S transponder/ADS-B transmitter [11].

8.2 Enhanced ADS-B Ground System OSA

8.2.1 Operational Hazard set definition

Inspection of the ADS-B RAD OSED and OSA Function Descriptions reveal that a number of differences existing between the Surveillance Functional model defined within the ADS-B RAD application and a model containing the WP15.4.5b Enhanced ADS-B Ground System. These differences include the integration of ADS-B data validation indications within the ADS-B Ground Receive Function, the presence of a WAM Ground Receive Function and the amalgamation of the Ground ADS-B Surveillance Processing Function and ADS-B to Radar association function within the SDPD Multi-Sensor Tracker [3].

The introduction of new functionality into the expanded Surveillance Functional Model has the potential to introduce new Operational Hazards into the ADS-B RAD OH set or at least introduce new failure causes for the current ADS-B RAD OH set, which should be assessed. The need to perform a new Operational Hazard assessment for a surveillance functional model incorporating the WP15.4.5 enhanced ADS-B ground system was discussed though several ad-hoc meetings organised between the author and Safety Subject Matter Experts from NATS and EUROCONTROL.

The Operational Hazard assessment activity is foreseen to comprise a workshop involving Safety Subject Matter Experts, ATC Experts and Flight Crew, as described between in Section OSA Step 1 - Operational Hazards identification .

8.2.2 Operational Hazard set Safety Objectives assessment

The new OH set should then have event trees developed for each OH, following the process described in Section OSA Step 2 – Hazard assessment and Severity Classification. The event tree branches developed for each OH can be used to determine the Severity of the analysed hazard, noting any Safety Requirements created at event tree barriers/branches.

Probability of Effect (Pe) values for each OH-OE pair can then be calculated using the process described within Section OSA Step 3 – Probability of effect and Safety Target determination. The final step within the first part of the OSA process is to select the most demanding Safety Objectives for each Operational Hazard using the assessed Safety Targets for the hazard Severity classes as input conditions.

8.2.3 Operational Hazard set Safety Requirements

The Safety Objectives defined for the each OH are used to develop Safety Requirements for the reference surveillance systems and enhanced ADS-B system, through the development of a fault tree for each OH (OSA Step 5 - Fault Tree Development).

Safety Objectives are then allocated to each branch of the fault tree, as described in Section OSA Step 6 - Safety Objective Allocation, leading to the Safety Requirement derivation for the enhanced ADS-B system and other surveillance scenario components e.g. reference radar system, reference WAM system, Surveillance Data Processing function, etc.

The resultant Safety Requirements set, complete with additional requirements input from the event and fault tree assessment process forms the full SR set which can be used to develop the Enhanced ADS-B Ground System and its constituent parts and add the ANSP in integrating the Enhanced ADS-B ground system into operational usage within their ATM system and for delivering ATS to controlled aircraft traffic.

9.0 References

[1] CARE/ASAS Activity 5 Description of a first package of GS/AS applications, Version 2.2

[2] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ADS-B-NRA APPLICATION, **ED-126**

[3] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ADS-B-RAD APPLICATION, **ED-161**

[4] GUIDELINES FOR APPROVAL OF THE PROVISION AND USE OF AIR TRAFFIC SERVICES SUPPORTED BY DATA COMMUNICATIONS, **ED-78A**

[5] SJU 15.04.05a Specification Baseline Document, **D17**

[6] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ATSA-ITP APPLICATION, **ED-159**

[7] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ENHANCED VISUAL SEPARATION ON APPROACH (ATSA-VSA), **ED-160**

[8] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS DOCUMENT FOR ENHANCED TRAFFIC SITUATIONAL AWARENESS DURING FLIGHT OPERATIONS (ATSA-AIRB), **ED-164**

[9] SJU 15.04.05a ADS-B 1090 MHz Ext. Squitter Ground Station Specification - Iteration 1, **D05**

[10] SJU 15.04.05a Interface Specifications for First Iteration, **D07**

[11] SJU 15.04.05a SDPD Specification – Iteration 1, **D06**

[12] METHODS TO PROVIDE SYSTEM-WIDE ADS-B BACK-UP, VALIDATION AND SECURITY White Paper, 1-4244-0378-2/06/$20.00 ©2006 IEEE

[13] Preliminary Safety Case for Air Traffic Control Service in Radar Areas using ADS-B Surveillance, PSC ADS-B-RAD, Edition 2.0

[14] **ESSAR 4** RISK ASSESSMENT AND MITIGATION IN ATM, Edition 1.0

[15] PROCESS FOR SPECIFYING RISK CLASSIFICATION SCHEME AND DERIVING SAFETY OBJECTIVES IN ATM, **ED-125**

[16] SJU 15.04.05a ADS-B Ground Surveillance Specifications for first iteration, **D18**

[17] SJU 15.4.5b First Iteration – Baseline Report/Matrix, **D02**

[18] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS FOR ADS-B FOR AIRPORT SURFACE SURVEILLANCE, **ED-163**

[19] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS FOR ATSA ON THE AIRPORT SURFACE, **ED-165**

[20] SAFETY, PERFORMANCE AND INTEROPERABILITY REQUIREMENTS FOR FLIGHT DECK INTERVAL MANAGEMENT (ASPA-FIM), **ED-195**

[21] Preliminary Safety Case for Airborne Traffic Situational Awareness for Enhanced Visual Separation on Approach, PSC ATSA-VSA Edition 2.1.

9.1 Use of copyright / patent material /classified material

No copyright/patent material is included in this specification.

10.0 Appendix A

Extract from 'CARE/ASAS Activity 4 - Review of ASAS Applications studied in Europe' document defining the Principle of Operation – Airborne Situation Assistance System or PO-ASAS application categories:

PO-ASAS category I

Airborne Traffic Situational Awareness applications*: These applications are aimed at enhancing the flight crews' knowledge of the surrounding traffic situation both in the air and on the airport surface, and thus improving the flight crew' s decision process for the safe and efficient management of their flight. No changes in separation tasks or responsibility are required for these applications.*

PO-ASAS category II

Airborne Spacing applications*: These applications require flight crews to achieve and maintain a given spacing with designated aircraft, as specified in a new ATC instruction. Although the flight crews are given new tasks, separation provision is still the controller's responsibility and applicable separation minima are unchanged.*

PO-ASAS category III

Airborne Separation applications*: In these applications, the controller delegates separation responsibility and transfers the corresponding separation tasks to the flight crew, who ensures that the applicable airborne separation minima are met. The separation responsibility delegated to the flight crew is limited to designated aircraft, specified by a new clearance, and is limited in time, space, and scope. Except in these specific circumstances, separation provision is still the controller's responsibility. These applications will require the definition of airborne separation standards.*

PO-ASAS category IV

Airborne Self-separation applications*: These applications require flight crews to separate their flight from all surrounding traffic, in accordance with the applicable airborne separation minima and rules of flight."*

END OF DOCUMENT -